

CLAIMS

1. An electronic certificate that has content data specifying an attribute delegation from an
5 identified issuer to a certificate subject, and an electronic signature for confirming the
content data; the content data including a condition requiring that a particular subject must
have a particular attribute in order for the delegation to be valid.
2. A certificate according to claim 1, wherein said certificate subject is generically any
10 subject whereby said attribute is delegated to any subject capable of showing said
condition to be satisfied, the particular subject of said condition being explicitly identified
in the content data.
3. A certificate according to claim 1, wherein said certificate subject is specifically
15 identified in the content data.
4. A certificate according to claim 3, wherein said particular subject is not separately
specified but is implicitly said specifically-identified certificate subject.
- 20 5. A certificate according to claim 3, wherein said particular subject is explicitly identified.
6. A certificate according to claim 1, including multiple said conditions in predetermined
logical relationship.
- 25 7. A certificate according to claim 6, wherein said logical relationship is explicitly stated.
8. A certificate according to claim 6, wherein said logical relationship is not explicit but is
implicitly an AND relationship.
- 30 9. A certificate according to claim 1 or claim 6, wherein said content data includes
certificate validity concerning at least one of:

- a date range identifying the period over which the certificate is valid;
 - the location of a certificate revocation list that should be checked before the certificate is used;
 - the location where a one-time use permission can be obtained or the certificate re-
- 5 validated;

said content data being structured into fields with the validity data and said condition or conditions being held in the same field.

10 **10.** A certificate according to any one of the preceding claims wherein the certificate has substantially the same form as an SPKI certificate with said condition or conditions being held in the validity field of the certificate.

11. Apparatus for generating a certificate of the form set out in any one of the preceding claims.

15 **12.** A reduction engine for combining certificates to establish a trust chain, at least comprising attribute delegations justified by certificates, that overall imparts a required attribute from a trusted issuer to a target subject, said reduction engine being operative upon using a certificate according to any one of claims 1 to 10 for justifying a delegation,

20 to establish a branch of said trust chain passing between said condition and a trusted issuer.

13. A trust chain discovery engine for finding a trust chain, at least comprising attribute delegations justified by certificates, that overall imparts a required attribute from a trusted issuer to a target subject, said reduction engine being operative upon using a certificate

25 according to any one of claims 1 to 10 for justifying a delegation, to establish a branch of said trust chain passing between said condition and a trusted issuer.